CCN-CERT **IA 14-20**

MARCO NORMATIVO Y SALVAGUARDAS

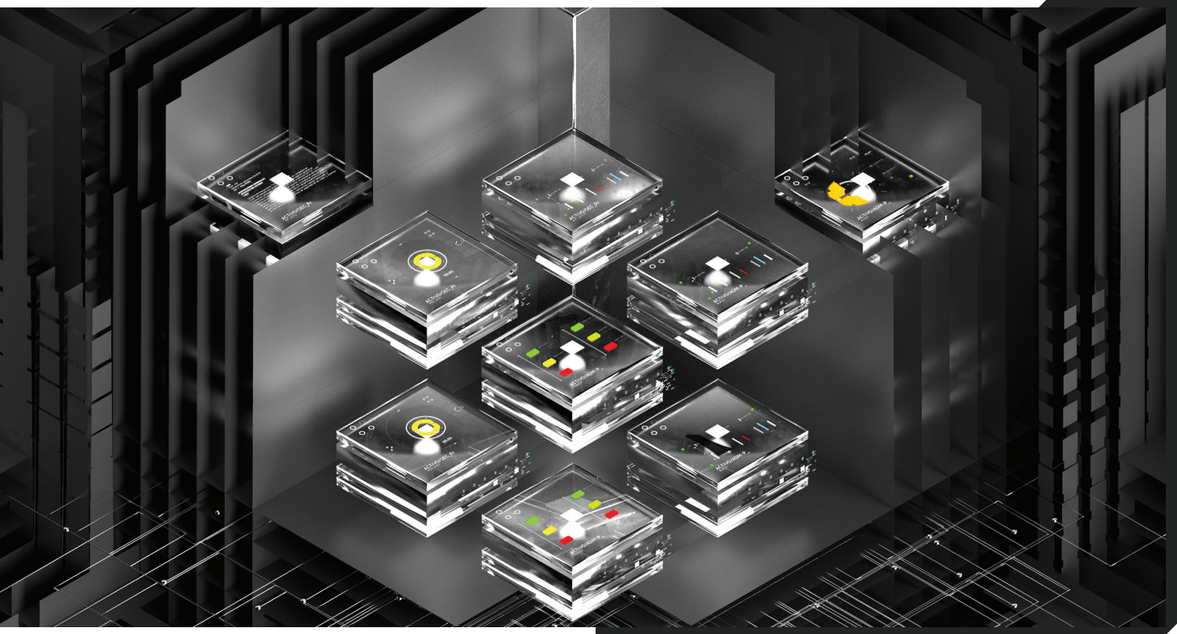
SEPTIEMBRE **2020**

CCN-CERT IA 14-20

INFORME ANUAL

CCN centro criptológico nacional

ccn-cert centro criptológico nacional



Edita:

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

Fecha de Edición: septiembre de 2020

Índice

1 Generalidades 02

Sobre el CCN-CERT 02
Contexto general 03

2 Resumen ejecutivo 04

3 Novedades en el contexto regulatorio 05

Estrategia Nacional de Ciberseguridad 2019 05
Reglamento sobre la Ciberseguridad *(Cybersecurity Act)* 05
Novedades relacionadas con el ENS 06
Otras disposiciones europeas 09
Otras disposiciones nacionales 10

4 Novedades en el contexto normativo, informes y guías 11

Servicios esenciales e infraestructuras críticas 11
Internet of Things 13
Protección de datos personales 14
Ciberseguridad 16
Servicios en Nube 18
Continuidad de negocio 19

5 Salvaguardas 20

Salvaguardas organizativas, normativas y procedimentales 20
Salvaguardas tecnológicas 23
Salvaguardas conductuales 33
Salvaguardas procedimentales 35

1 Generalidades

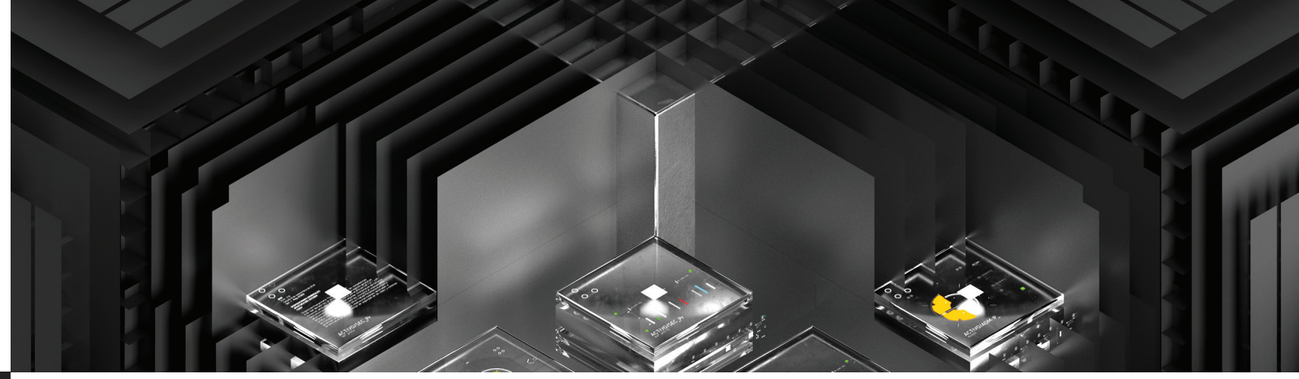
1.1 Sobre el CCN-CERT

El **CCN-CERT** es la **Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional**, **CCN**, adscrito al **Centro Nacional de Inteligencia**, **CNI**. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier Organismo o empresa pública. En el caso de operadores críticos del sector público la **gestión de ciberincidentes** se realizará por el **CCN-CERT** en coordinación con el **CNPIC**.

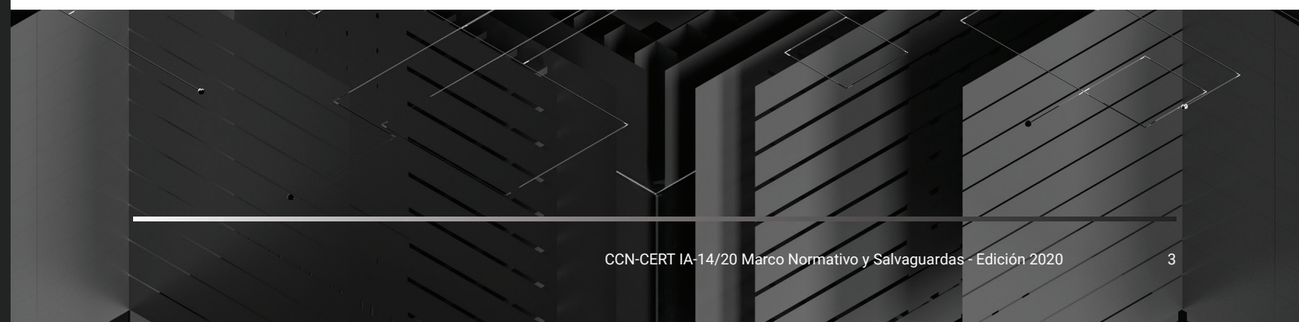


1.2 Contexto general

La **seguridad de la información** y la **ciberseguridad** se han convertido en una de las principales preocupaciones tanto de las **Administraciones Públicas** como de las **organizaciones privadas**. La cada vez mayor frecuencia de los incidentes en el mundo digital y el impacto que estos tienen está poniendo en evidencia que ninguna organización, sea cual sea su tamaño o naturaleza, escapa a la amenaza de un ciberataque. Un impacto que puede afectar a su imagen reputacional o a la continuidad de sus servicios, y, por tanto, a su propia existencia, en función de su tamaño y de cómo se haya preparado para ello.

En este sentido, la gestión de la ciberseguridad de las organizaciones debe estar totalmente alineada con la criticidad de sus procesos, sin perder de vista que la ciberseguridad no contempla únicamente aspectos técnicos, sino también organizativos, normativos y legales.

Para ello, resulta fundamental que las **salvaguardas tecnológicas** estén coordinadas e integradas en una capa organizativa que contemple aquellos aspectos complementarios a la tecnología, necesarios para asegurar que la ciberseguridad y la seguridad de la información se entienden como un proceso horizontal dirigido a garantizar la **ciberresiliencia** de los procesos de negocio. También es necesaria la existencia de un entramado legal que garantice la disponibilidad de los servicios esenciales para el funcionamiento de un país y la protección de la sociedad y los derechos fundamentales de sus ciudadanos.



2 Resumen ejecutivo

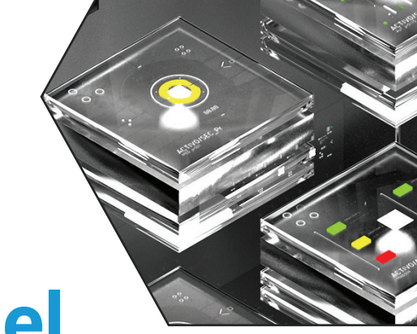
En España existe ya un consolidado marco regulatorio y normativo, desarrollado a instancias de la **Unión Europea** o a iniciativa propia, dirigido a regular cómo las organizaciones deben proteger las infraestructuras tecnológicas que gestionan, los procesos que sobre ellas se desarrollan y la información que tratan, iniciativas nacionales que incluso en algunos casos han constituido un referente a nivel internacional en la materia.

En el contexto internacional, la **ciberseguridad** es una de las principales prioridades políticas tanto para la **Unión Europea** como para la **OTAN**, organismos a los que pertenece España. Desde ambas organizaciones se está trabajando activamente para homogeneizar las capacidades y el nivel de madurez de la ciberseguridad de sus estados miembros.

En paralelo, múltiples organismos internacionales han venido publicando referenciales y nuevos estándares con propuestas de normalización de los nuevos aspectos relacionados con la ciberseguridad, como se detalla más adelante.

Además, el nuevo escenario que ha provocado la pandemia de la covid-19 en el contexto tecnológico mundial con el **teletrabajo** plantea a su vez nuevos escenarios de riesgo para las organizaciones. La ampliación del dominio protegible y por tanto la mayor superficie de exposición a nuevos vectores de ataque, la revisión "forzada" de sus planes de contingencia y de continuidad de negocio, las controversias en cuanto a la protección de los datos personales relacionados con la salud de los ciudadanos en general y de los empleados en particular, el aumento del uso de equipos personales o particulares para acceder a recursos corporativos, la aplicación de medidas de seguridad a esos entornos domésticos y la posible monitorización de los mismos al conectarlos con los entornos corporativos, la "nuevas responsabilidades" de las personas jurídicas en estos nuevos escenarios tecnológicos, etc., seguro que provocarán muchos cambios en el marco regulatorio y normativo existente que regula el ecosistema de la ciberseguridad.

En cualquier caso, sin perder de vista el marco vigente preexistente, y aunque es imposible incluirlas todas, a continuación, se relacionan las principales novedades que 2019 ha traído en materia legal y normativa en diferentes contextos que se han considerado relevantes. Dadas las fechas en que se publica este informe, se ha incluido también alguna novedad relevante publicada durante el primer semestre de 2020.



3 Novedades en el contexto regulatorio

3.1 Estrategia Nacional de Ciberseguridad 2019[1]

Estrategia Nacional de Ciberseguridad

El 30 de abril de 2019, el **Boletín Oficial del Estado** recogía la **Orden PCI/487/2019**, de 26 de abril, por la que se publicaba la **Estrategia Nacional de Ciberseguridad 2019**, aprobada por el **Consejo de Seguridad Nacional** en su reunión del 12 de abril.

Dicha estrategia, alineada con la **Estrategia de Seguridad Nacional de 2017**, establece un esquema novedoso en el ámbito de la ciberseguridad, con **cinco (5) objetivos generales** transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la seguridad en España.

El Centro Nacional de Inteligencia participó activamente en la elaboración de esta Estrategia. No en vano, desde sus orígenes en 2014, ha ocupado la presidencia del Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional, coordinador de los organismos con competencia en la materia a nivel nacional.

3.2 Reglamento sobre la Ciberseguridad (*Cybersecurity Act*)[2]

Cybersecurity Act

El **Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo**, de 17 de abril de 2019, surge con el objetivo de ampliar la respuesta de la Unión Europea a los ataques cibernéticos, mejorar su resiliencia y aumentar la confianza en el **Mercado Único Digital**.

Dicho reglamento tiene además como **objetivos fortalecer a la Agencia Europea de Ciberseguridad (ENISA)**, para así mejorar la **coordinación y la cooperación en materia de ciberseguridad** en todos los Estados miembro de la UE y entre instituciones, agencias y organismos; y establecer un marco de certificación de ciberseguridad de la Unión Europea que

1 Véase https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf
2 Véase https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=es

permita el surgimiento de esquemas de certificación particularizados para categorías específicas de productos, procesos y servicios de TIC.

El **CCN**, como **Autoridad Nacional de Certificación de la Ciberseguridad**, conforme al citado Reglamento, supervisará la correcta implementación de los esquemas europeos de certificación en España, garantizando la validez de los certificados emitidos en nuestro país.

En este sentido, a principios de 2020, el CCN ha comenzado a desarrollar una nueva serie de **Guías CCN-STIC**. En este caso, se trata de la serie 2000[3], cuyo objetivo es recoger todas aquellas guías, procedimientos y formularios del **Organismo de Certificación**, con la finalidad de facilitar los procesos de evaluación y certificación del **Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información**.

Las **Series CCN-STIC** son normas, instrucciones, guías y recomendaciones desarrolladas por el CCN, con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.

3.3 Novedades relacionadas con el ENS

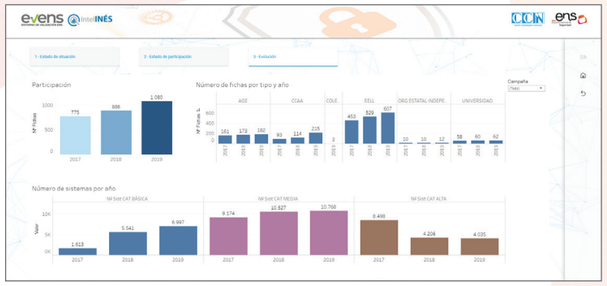
El **Esquema Nacional de Seguridad** ha supuesto un hito en materia de ciberseguridad en España y un referente para otros países. Pero en un entorno tan cambiante como este, debe mantenerse en continua revisión y adaptación a los nuevos retos y tendencias que se avecinan, reduciendo en lo posible las vulnerabilidades y promoviendo la defensa activa.

Esquema Nacional de Seguridad

3 Véase https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/2000-organismo-certificacion.html

En relación con el ENS, durante 2019 se han producido las siguientes **novedades**:

Informe Nacional del Estado de Seguridad (INES)[4]



Elaborado por el CCN, el Informe del Estado de Seguridad de 2019 fue publicado el 1 de mayo de 2020, aunque sus resultados generales fueron adelantados durante las jornadas STIC en diciembre de 2019.

Su **objetivo** es **facilitar** a todos los organismos la **obtención de un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas**. A través de asistentes de seguridad, INES permite la recogida de información organizada, delegada y supervisada sobre los equipos de una organización.

Entorno de Validación del Esquema Nacional de Seguridad (EVENS)[5]

A modo de red neuronal, este entorno proporciona una **vía de entrada común a toda la documentación elaborada y relacionada con el ENS**: Informes del Estado de Seguridad, normativa, ITS, Guías Serie 800 (ENS), Abstract, etc.

e-vens ENTORNO DE VALIDACIÓN ENS

Uno de sus objetivos es capacitar en el ENS y aportar conocimiento, tanto en el proceso de Conformidad, como en el de Adecuación al Esquema, así como en la elaboración de la Declaración de Aplicabilidad y Perfiles de Cumplimiento Específicos.

Responsabilidades y Funciones en el ENS[6]

Publicada en abril de 2019, la **guía CCN-STIC 801 Esquema Nacional de Seguridad. Responsabilidad y Funciones** tiene por objeto recoger las responsabilidades generales en la gestión de la seguridad de los sistemas de información de las entidades del Sector Público del ámbito subjetivo de aplicación del ENS.

Esta actualización de la guía original, publicada en 2010, viene a revisar la definición de la estructura de seguridad, actores y responsabilidades asociadas a los mismos que se recomendaba originalmente. Por último, y como principales novedades, incluye un epígrafe dedicado a la gestión de los riesgos y otro a la concurrencia del ENS con el Reglamento General de Protección de Datos (RGPD).

4 Véase https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/10055-la-solucion-ines-de-nuevo-disponible-para-la-gestion-de-la-seguridad-con-importantes-novedades.html

5 Véase https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/evens

6 Véase https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

Perfiles de cumplimiento específicos para entornos *cloud*

Con el fin de permitir a aquellas entidades comprendidas en el ámbito de aplicación del ENS que utilizan sistemas basados en *cloud* alcanzar una mejor y más eficiente adaptación al mismo, el CCN ha validado y publicado en diciembre de 2019 los **perfiles de cumplimiento específicos para los siguientes entornos**:

- Azure Servicio de Cloud Corporativo (Guía CCN-STIC 884)[7]
- Office 365 Servicio de Cloud Corporativo (Guía CCN-STIC 885)[8]
- Sistemas Cloud Privados y Comunitarios (Guía CCN-STIC 886)[9]

Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 3/2010, de 8 de enero, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

Obligaciones de los prestadores de servicios a las entidades del sector público[10]

Elaborado por el CCN y publicado en junio de 2020, este documento recoge las obligaciones que en materia de ciberseguridad y seguridad de la información deben cumplir las empresas públicas y privadas que prestan servicios a entidades públicas, cuando dichos servicios están sujetos al cumplimiento del ENS.

Informes CoCENS[11]

El CCN-CERT ha procedido a publicar guías bajo la taxonomía de informe **CCN-CERT IC**, que comprende los informes elaborados por el Consejo de Certificación del ENS (**CoCENS**).

Entre los recientemente publicados, se encuentra la Guía *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*[12] cuyo objeto es servir de referencia y establecer los criterios generales para la Auditoría y Certificación de los sistemas de información del ámbito de aplicación del Esquema Nacional de Seguridad, especialmente los dirigidos a las Entidades de Certificación del ENS.

7 Véase https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4572-ccn-stic-884-perfil-de-cumplimiento-especifico-azure/file.html

8 Véase https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4575-ccn-stic-885-perfil-de-cumplimiento-especifico-office-365/file.html

9 Véase https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4578-ccn-stic-886-perfil-de-cumplimiento-especifico-de-cloud-privados/file.html

10 Véase https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/257-abstract-obligaciones-de-los-prestadores-de-servicios-a-las-entidades-publicas/file

11 Véase https://www.ccn-cert.cni.es/guias/informes-cocens.html

12 Véase https://www.ccn-cert.cni.es/pdf/guias/informes-cocens/3818-ccn-cert-ic-01-19-criterios-generales-auditorias/file.html

3.4 Otras disposiciones europeas

Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo relativa a los datos abiertos y su reutilización en el sector público[13]

Esta directiva tiene por finalidad afrontar los obstáculos derivados de una amplia reutilización de la información del sector público en toda la Unión, y actualizar el marco legislativo con los avances en las tecnologías digitales, estimulando la innovación digital, en especial en lo que respecta a inteligencia artificial.

Nuevo protocolo de la Unión Europea para protegerse frente a los ciberataques[14]

Este protocolo adoptado por el Consejo de la Unión Europea otorga un papel central al **Centro Europeo de Delitos Cibernéticos (EC3) de Europol**, y es parte del **Anteproyecto de la UE** para la respuesta coordinada a incidentes y crisis de ciberseguridad transfronterizas a gran escala. Sirve como una herramienta para ayudar a las autoridades policiales de la Unión Europea a proporcionar una respuesta inmediata a los principales ataques cibernéticos transfronterizos haciendo uso de una evaluación rápida, el intercambio seguro y oportuno de información crítica y la coordinación efectiva de los aspectos internacionales de sus investigaciones.

Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo sobre Derechos de autor[15]

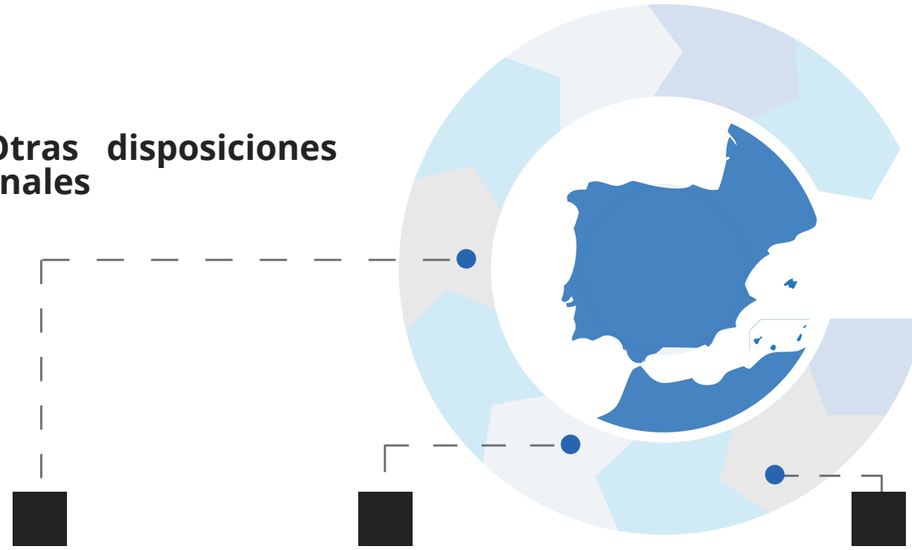
Establece normas destinadas a armonizar el **Derecho de la Unión** en el ámbito de los derechos de autor y derechos afines en el marco del mercado interior, teniendo especialmente en cuenta los usos digitales y transfronterizos de los contenidos protegidos. Establece asimismo normas sobre excepciones y limitaciones a los derechos de autor y derechos afines, sobre facilitación de licencias, así como normas destinadas a garantizar el correcto funcionamiento del mercado de explotación de obras y otras prestaciones.

13 Véase https://www.boe.es/doue/2019/172/L00056-00079.pdf

14 Véase https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks

15 Véase https://www.boe.es/doue/2019/130/L00092-00125.pdf

3.5 Otras disposiciones nacionales



Real Decreto-ley 14/2019, de 31 de octubre[16]

El real decreto-ley, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, tiene por objeto regular medidas relativas a la documentación nacional de identidad, la identificación electrónica ante las Administraciones Públicas, os datos que obran en poder de las Administraciones Públicas, la contratación pública y al sector de las telecomunicaciones y la coordinación de la ciberseguridad del sector público.

Ley 2/2019 de propiedad Intelectual (modificación)[17]

Esta ley modifica el texto refundido de la **Ley de Propiedad Intelectual**, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

Código de Derecho de la Ciberseguridad[18]

Aunque no es una novedad de 2019, se considera relevante hacer constar la existencia de este código que aglutina, de manera actualizada, las normas que afectan directamente a la ciberseguridad, y facilita a empresas, instituciones públicas, profesionales y ciudadanos en general el compendio de la legislación que regula esta materia y que resulta fundamental para su adecuada protección.

16 Véase https://www.boe.es/eli/es/rdl/2019/10/31/14/dof/spa/pdf
17 Véase https://www.boe.es/boe/dias/2019/03/02/pdfs/BOE-A-2019-2974.pdf
18 Véase https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=2&nota=0

4 Novedades en el contexto normativo, informes y guías

4.1 Servicios esenciales e infraestructuras críticas

Guía nacional de notificación y gestión de ciberincidentes[19]

Elaborada por el **Consejo de Ciberseguridad Nacional** y publicada el 9 de marzo de 2019, esta guía pretende servir de marco de referencia para la notificación y gestión de ciberincidentes en el contexto de las Administraciones Públicas, las infraestructuras críticas y los operadores de servicios esenciales.

Guía para la contratación de productos y servicios de seguridad en entornos hospitalarios[20]

Este informe de ENISA ofrece directrices de ciberseguridad para los hospitales a la hora de adquirir servicios, productos e infraestructura. Todas las buenas prácticas están vinculadas a los tipos de adquisición para los que son pertinentes y a las amenazas que pueden mitigar, proporcionando un conjunto de prácticas fáciles de filtrar para aquellos hospitales que deseen centrarse en aspectos concretos.

MDCG 2019-16 Guía de ciberseguridad para dispositivos médicos[21]

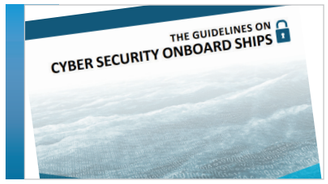
Este documento ha sido aprobado por el **Grupo de Coordinación de Dispositivos Médicos (MDCG)**.

Aunque se trata de un documento de trabajo que no refleja ninguna postura oficial de la Comisión Europea, se ha considerado relevante incluirlo, pues trata temas como los requisitos de ciberseguridad tanto en el proceso de fabricación de los dispositivos como en su posterior uso seguro en los hospitales, la legislación de aplicación o el mapeo con algunos de los requisitos de la **Directiva NIS**.

19 Véase https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf
20 Véase https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services/at_download/fullReport
21 Véase https://ec.europa.eu/docsroom/documents/38941/attachments/1/translations/en/renditions/native

Buenas prácticas en ciberseguridad en el sector marítimo[22]

Elaborado por ENISA en colaboración con varios puertos de la Unión Europea y publicado en noviembre de 2019, este informe pretende proporcionar una base sobre la que los CIO y los CISO de las entidades que participan en el ecosistema portuario, especialmente las autoridades portuarias y los operadores de terminales, puedan elaborar su estrategia de ciberseguridad. En el documento se analizan los **riesgos** específicos **del ámbito portuario** y se describen los principales **escenarios de ciberataque** que podrían afectarles.



Directrices de ciberseguridad en el transporte marítimo[23]

El anterior informe cubre los riesgos presentes en las instalaciones portuarias, pero también hay que contemplar los riesgos específicos del transporte marítimo. En los **buques** conviven **sistemas IT** y **sistemas OT**, muchas veces en las mismas redes, y la digitalización, la integración y la automatización introducen cada vez más riesgos que pueden poner en peligro la ciberseguridad de estas infraestructuras.

Esta guía, elaborada de manera conjunta por un grupo de organizaciones de transporte marítimo internacional, pretende servir de referencia para gestionar adecuadamente la ciberseguridad en un contexto tan específico como es el transporte marítimo.

Programa de Seguridad CSP de SWIFT versión 2019[24]

La **Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales** (SWIFT, Society for Worldwide Interbank Financial Telecommunication) publicó en 2019 su **programa de seguridad de clientes** (CSP, Customer Security Programme).

Este programa, que tiene dos versiones, es de obligado cumplimiento para todas las entidades financieras que forman parte de dicha organización, y su cumplimiento debe ser reportado de manera formal desde este mismo año.

22 Véase https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport

23 Véase https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

24 Véase https://www.swift.com/myswift/customer-security-programme-csp_/security-controls/2019

4.2 Internet de las Cosas[25]

Buenas prácticas para la seguridad de vehículos inteligentes[26]

El año pasado ENISA publicó el documento ***ENISA good practices for security of Smart Cars***, un informe que define las buenas prácticas para la seguridad de los automóviles inteligentes (vehículos conectados y autónomos o semiautónomos), que se caracterizan por sus prestaciones orientadas a mejorar la experiencia de los usuarios.

Este documento tiene como propósito servir como punto de referencia para promover la ciberseguridad de este tipo de automóviles, elevando el nivel de conciencia sobre las amenazas y riesgos relevantes con un enfoque en la "*cybersecurity for safety*".

ISO/SAE 21434 Vehículos de carretera – Ingeniería de ciberseguridad[27]

La **Organización Internacional de Estandarización** (ISO) y la **Sociedad de Ingenieros Automotrices** (SAE International, Society of Automotive Engineers) están colaborando en la definición de un **estándar** que homogenice los **requisitos de ciberseguridad** que deben cumplir todos los actores que forman parte de la industria de fabricación de coches.

El enfoque de este estándar iría orientado a cubrir todas las fases del ciclo de vida de la fabricación, incluidos los requisitos de diseño, ingeniería, especificaciones para proveedores, implementación, prueba y operaciones, y contemplando subsistemas, componentes, conexiones y software. Se espera que la norma sea publicada durante 2020.

Proyecto de ley sobre ciberseguridad en IoT en EEUU[28]

Este proyecto de ley establece que el **Instituto Nacional de Estándares y Tecnología estadounidense** (NIST, National Institute of Standards and Technology) defina medidas específicas para aumentar la ciberseguridad de los dispositivos IoT.

Entre otras, contempla la definición de **recomendaciones** para el uso y la gestión adecuados de los **dispositivos IoT** que son propiedad o están controlados por el gobierno norteamericano, incluidos los requisitos mínimos de seguridad de la información para la gestión de los riesgos de ciberseguridad, así como la publicación de directrices sobre políticas y procedimientos para la presentación de informes, coordinación y comunicación de posibles vulnerabilidades identificadas. Se prevé que el proyecto sea aprobado durante 2020.

25 *Internet of Things*

26 Véase https://www.enisa.europa.eu/publications/smart-cars

27 Véase https://www.iso.org/standard/70918.html

28 Véase https://www.congress.gov/bill/116th-congress/senate-bill/734?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+Act+of+2019%22%5D%7D&r=1

4.3 Protección de datos personales

ISO/IEC 27701:2019 Gestión de la información de privacidad[29]

Con la entrada en vigor del **Reglamento General de Protección de Datos (RGPD)**, y su posterior adaptación a la legislación española con la **Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)**, se incluyó la posibilidad de ayudar a empresas y organizaciones a verificar que cumplen con las leyes y demostrar el principio de responsabilidad proactiva (art. 24 del RGPD) a través de estándares o recomendaciones, así como certificaciones.

Como norma de sistema de gestión internacional, su objetivo es proporcionar orientación sobre la protección de la privacidad, incluida la forma en que las organizaciones deben gestionar la información personal, además de ayudar a demostrar el cumplimiento de la normativa en privacidad, como el RGPD, en todo el mundo.

ISO/IEC 29184:2020 Aviso de privacidad online y consentimiento[30]

La norma pretende definir los requisitos para garantizar el derecho de información y la adecuada obtención de consentimientos relacionados con la recopilación y el uso de los datos personales y de actividad de los usuarios en el contexto de los servicios online.

29 Véase https://www.iso.org/standard/71670.html
30 Véase https://www.iso.org/standard/70331.html

Guía AEPD sobre el uso de las cookies[31]

En noviembre de 2019 la **Agencia Española de Protección de Datos** publicó una guía con soluciones y orientaciones propuestas para cumplir con las obligaciones previstas en la Ley 34/2002 de **Servicios de la Sociedad de la Información y del Comercio Electrónico** (LSSICE), el **Reglamento Europeo 2016/679 de Protección de Datos Personales** (RGPD) y la L**ey Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales** (LOPDGDD).

Guía AEPD para las Evaluaciones de Impacto en la Protección de Datos[32]

La AEPD ha elaborado la presente guía con el objetivo de promover una **cultura proactiva de la privacidad**, facilitando la realización de las Evaluaciones de Impacto en la Protección de Datos, y proporcionando de esta manera un marco de referencia para el ejercicio de esta obligación que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas.

Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial[33]

Este documento elaborado por la AEPD aborda las inquietudes que el uso de esta tecnología genera en relación con la protección de los datos personales, y repasa los aspectos más importantes que deben tenerse en cuenta a la hora de diseñar productos y servicios que lleven a cabo tratamientos de datos que incluyan **Inteligencia Artificial** (IA).

31 Véase https://www.aepd.es/sites/default/files/2019-12/guia-cookies_1.pdf
32 Véase https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf
33 Véase https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

4.4 Ciberseguridad

Innovación en ciberseguridad desde las estrategias nacionales europeas[34]

Integrado en uno de los objetivos de ENISA, que es incrementar y homogeneizar el nivel de madurez en ciberseguridad en la Unión Europea, este informe, publicado en noviembre de 2019, analiza cómo están innovando y qué nuevas iniciativas están integrando en sus estrategias nacionales de ciberseguridad cada uno de los Estados miembros de la Unión Europea.

WEF Guía de ciberseguridad para líderes en el mundo digital[35]

Con la **ciberresiliencia** como gran protagonista en las estrategias de las organizaciones en materia de ciberseguridad para los próximos años, esta guía del **World Economic Forum** propone una serie de principios clave a cubrir desde la dirección en las organizaciones, con el objetivo de generar un contexto de confianza, seguridad y estabilidad para sus procesos de negocio en el contexto del mercado único digital.

NIST SP 800-37 Risk Management Framework Rev 2[36]

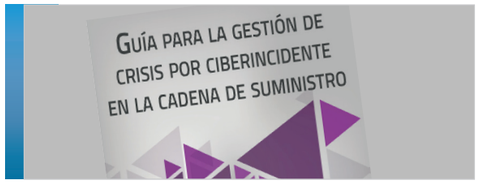
El documento **NIST SP 800-37 Revisión 2**, publicado por el **Instituto Nacional de Estándares y Tecnología estadounidense**, propone un marco de gestión de riesgos, y proporciona a las organizaciones directrices para implantar un proceso flexible de gestión de los riesgos de seguridad y privacidad relacionados con sus sistemas de información.

Es la primera publicación del NIST que aborda la gestión de los **riesgos de seguridad y privacidad** en una metodología integrada y aplicable a cualquier sector, organización o tipo de sistema. La actualización incluye una alineación con los principios del Cybersecurity Framework del NIST (NIST CSF), la integración de los procesos de gestión de los riesgos para la privacidad, una alineación con los procesos de ingeniería de seguridad del ciclo de vida del sistema y la incorporación del riesgo de la cadena de suministro en los procesos de gestión.

34 Véase https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1/at_download/fullReport

35 Véase http://www3.weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf

36 Véase https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf



Guía para la Gestión de Crisis por Ciberincidente en la cadena de suministro[37]

La Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum), con el apoyo del Departamento de Seguridad Nacional (DSN), el Centro Criptológico Nacional (CCN), el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), el Instituto Nacional de Ciberseguridad (INCIBE) y la Agència de Ciberseguretat de Catalunya ha publicado esta guía, que analiza uno de los contextos que está cogiendo más relevancia en la gestión de la ciberseguridad de las organizaciones: la gestión de la misma en los procesos que tienen externalizados.

La guía responde a la necesidad de contar con **mecanismos de respuesta a ciberincidentes** que tengan en cuenta el incremento en la dependencia de terceros, y por tanto el aumento de la superficie de exposición a incidentes, y pone en valor la importancia de la seguridad en toda la cadena de suministro, aspecto que en determinados contextos tiene incluso una responsabilidad legal, como es en el caso de los prestadores de servicios esenciales.

ISO/IEC 27102:2019 Gestión de seguridad de la información – Guía para ciberseguros[38]

Publicada en agosto de 2019, la norma ISO/IEC 27102:2019 ofrece una guía para analizar cuándo tiene sentido contemplar la contratación de un ciberseguro en el plan de tratamiento de riesgos de una determinada amenaza y, en su caso, cómo establecer la relación de compartición de riesgos entre la compañía aseguradora y el asegurado dentro de la estrategia de ciberseguridad de la organización.

37 Véase https://www.ismsforum.es/noticias/1542/isms-forum-publica-la-guia-para-la-gestion-de-crisis-por-ciberincidente-en-la-cadena-de-suministro/

38 Véase https://www.iso.org/standard/72436.html

4.5 Servicios en Nube

Como se ha reflejado en el apartado correspondiente al ENS, el CCN está desarrollando **perfiles de cumplimiento específicos** para establecer las medidas de seguridad específicas para sistemas basados en la nube en el ámbito de aplicación del ENS.

En el contexto específico de la **seguridad en entornos cloud** existen referenciales ya conocidos como el estándar **ISO/IEC 27017** Controles de Seguridad para Servicios Cloud o la Cloud Control Matrix (CCM) de la Cloud Security Alliance.

En 2019 se han publicado las siguientes **novedades**, que se detallan aquí por ser específicos para **entornos en la nube**.

ISO/IEC 27018:2019 Protección de datos personales en la nube[39]

La norma **ISO/IEC 27018:2019** es un código de prácticas diseñado para **proteger información personalmente identificable** (PII) en la nube, dirigida principalmente a empresas que juegan el rol de encargado de tratamiento (*PII processors*) en la prestación de servicios de procesamiento de datos personales por medio de computación en la nube para otras organizaciones.

ISO/IEC 19086-4:2019 SLA Cloud computing– Componentes de seguridad y protección de datos personales[40]

La **serie ISO/IEC 19086 (1-4)** está dirigida a **estandarizar** los acuerdos de nivel de servicio entre los proveedores de servicios cloud y sus clientes. En su parte 4, publicada en 2019, se especifican los **requisitos de seguridad y de protección** de los datos personales que pueden tener relación con los acuerdos de nivel de servicio.

39 Véase https://www.iso.org/standard/76559.html
40 Véase https://www.iso.org/standard/68242.html

4.6 Continuidad de negocio

Una de las principales consecuencias que en el contexto de las tecnologías de la información y las comunicaciones ha tenido la pandemia mundial de la covid-19 ha sido el hecho de que las organizaciones se han dado cuenta de la importancia de contar con **planes de contingencia y planes de continuidad de negocio** que realmente respondan a las necesidades de sus procesos de negocio, tanto desde el punto de vista de sus infraestructuras tecnológicas como desde el punto de vista del acceso a sus instalaciones y de la disponibilidad de las personas encargadas de llevar a cabo esos procesos.

Este hecho va a provocar que las organizaciones identifiquen de manera prioritaria la necesidad de **revisar, actualizar** y **probar la efectividad** de esos planes. En esta materia, el estándar de facto es la norma internacional **ISO 22301**, que determina los **requisitos** que deben contemplar los sistemas de gestión de continuidad de negocio para garantizar la disponibilidad y la resiliencia de los procesos críticos de negocio.

Aunque no ha traído cambios drásticos sobre la versión de 2012, en octubre de 2019 se publicó una revisión de la norma.[41]

41 Véase https://www.iso.org/standard/75106.html

5 Salvaguardas

5.1 Salvaguardas organizativas, normativas y procedimentales

La construcción de la seguridad de la información pasa, en primera instancia, por disponer de los **elementos organizativos, normativos** y **procedimentales necesarios**. Para ello, cada organización involucrada en el desarrollo y mantenimiento de un proceso de seguridad de la información debe haber redactado y aprobado la siguiente **batería de herramientas normativas**.

Política de Seguridad de la Información

Normativa Interna

Procedimientos de Seguridad

Se describe seguidamente el contenido esencial de cada uno de tales componentes.

Política de Seguridad de la Información[42]:

En líneas generales, una **Política de Seguridad de la Información** es un conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que la organización gestiona y protege la información y los servicios que, sustentados en sistemas de información, constituyen sus competencias o funciones; conteniendo, entre otras cuestiones, la **misión u objetivos de la entidad**, su **marco normativo**, la **organización de la seguridad de la información**, la **política de concienciación y formación**, la **gestión de los riesgos** y su propio **proceso de revisión**.

Además de ello, la Política de Seguridad de la Información debe detallar las **atribuciones** de cada departamento, unidad o persona responsable del mantenimiento de la seguridad, así como los preceptivos mecanismos de coordinación y resolución de conflictos[43].

La importancia capital de la Política de Seguridad de la Información, como base esencial para la construcción de la seguridad de la Información, hace que constituya siempre el primer elemento que debe acometerse, debiendo ser públicamente aprobada por su órgano directivo, como evidencia del compromiso de la organización con la seguridad de la información y su mantenimiento[44].

Normativa interna[45]:

Dado que la Política de Seguridad es un documento de alto nivel, es necesario desarrollarla con documentos más precisos que ayuden a llevar a cabo lo propuesto, que materialicen sus requisitos mínimos y que suelen comprender: la organización e implantación del proceso de seguridad; el análisis y gestión de los riesgos; la gestión de personal; las características de la profesionalidad exigida, interna o externamente, entre otras cuestiones.

Por tanto, se puede decir que las **Normas de Seguridad de la Información** uniformizan el uso de aspectos concretos del sistema, indican el uso correcto y las responsabilidades de los usuarios y, al tratarse de normas de obligatorio cumplimiento, deben ser asimismo aprobadas y adecuadamente difundidas por el órgano directivo de la organización[46].

De entre ellas, la más importante, siguiendo lo dispuesto por la Política de Seguridad de la Información de la organización, es la **Normativa interna del uso de los medios electrónicos,** gestionados o bajo la responsabilidad de la entidad, que señalará los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

42 Se corresponde con la medida [org.1] del Anexo II del ENS.
43 Véase Guía CCN-STIC 801 ENS: Responsabilidades y Funciones.
44 Véase Guía CCN-STIC 805 ENS: Política de Seguridad de la Información.
45 Se corresponde con la medida [org.2] del Anexo II del ENS.
46 Véase Guía CCN-STIC 821 Normas de Seguridad.

Procedimientos de seguridad[47]:

Finalmente, para completar el marco normativo, cada entidad inmersa en la implantación y mantenimiento de un proceso de seguridad de la información debe disponer de un conjunto documental de **Procedimientos de Seguridad** que aborden cómo han de realizarse tareas concretas, indicando, paso a paso, el proceder deseable en cada caso, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

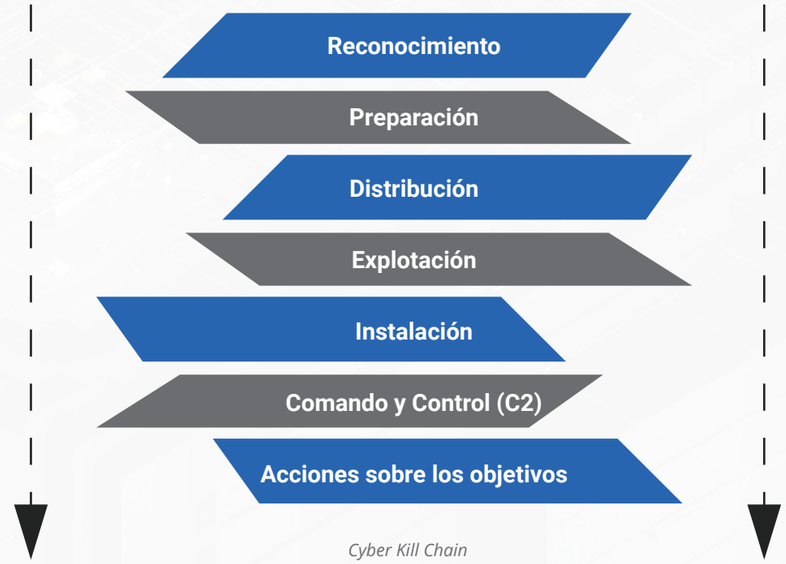
Aunque cada procedimiento de seguridad deberá estar alineado con la medida de seguridad que desarrolla y que, por lo tanto, será dependiente del nivel de seguridad requerido, a modo de ejemplo, se señalan algunos de los **procedimientos de seguridad** más habituales: Procedimiento de Arquitectura de Seguridad de los sistemas; Procedimiento para la adquisición de nuevos componentes; Procedimiento de Gestión de Usuarios; Procedimiento de Control de Seguridad en la Operativa; Procedimiento de Gestión del Mantenimiento; Procedimiento de formación y concienciación; Procedimiento de protección de equipos móviles; entre otros.

En el caso del **Esquema Nacional de Seguridad**, cada uno de los procedimientos estará vinculado a una o más medidas de seguridad de su **Anexo II**, siendo objeto, en su caso, de la preceptiva **Auditoría de Seguridad**.

47 Se corresponde con la medida [org.3] del Anexo II del ENS.

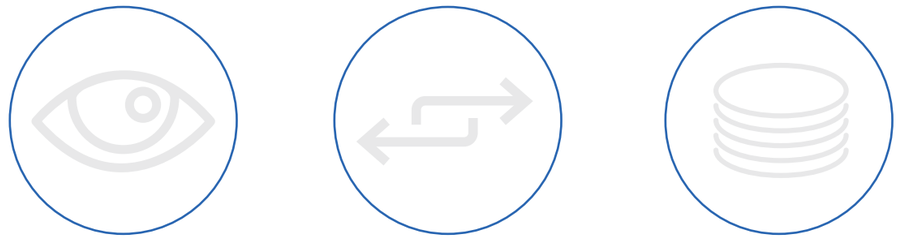
5.2 Salvaguardas tecnológicas

Antes de pasar a describir las principales salvaguardas tecnológicas, y para dotarlas de contexto, es importante repasar brevemente el **ciclo de vida** de la mayoría de las **ciberamenazas**, modelo desarrollado por Lockheed Martin y denominado Cyber Kill Chain®[48]. A continuación, puede verse un diagrama de sus **fases**:



Cyber Kill Chain

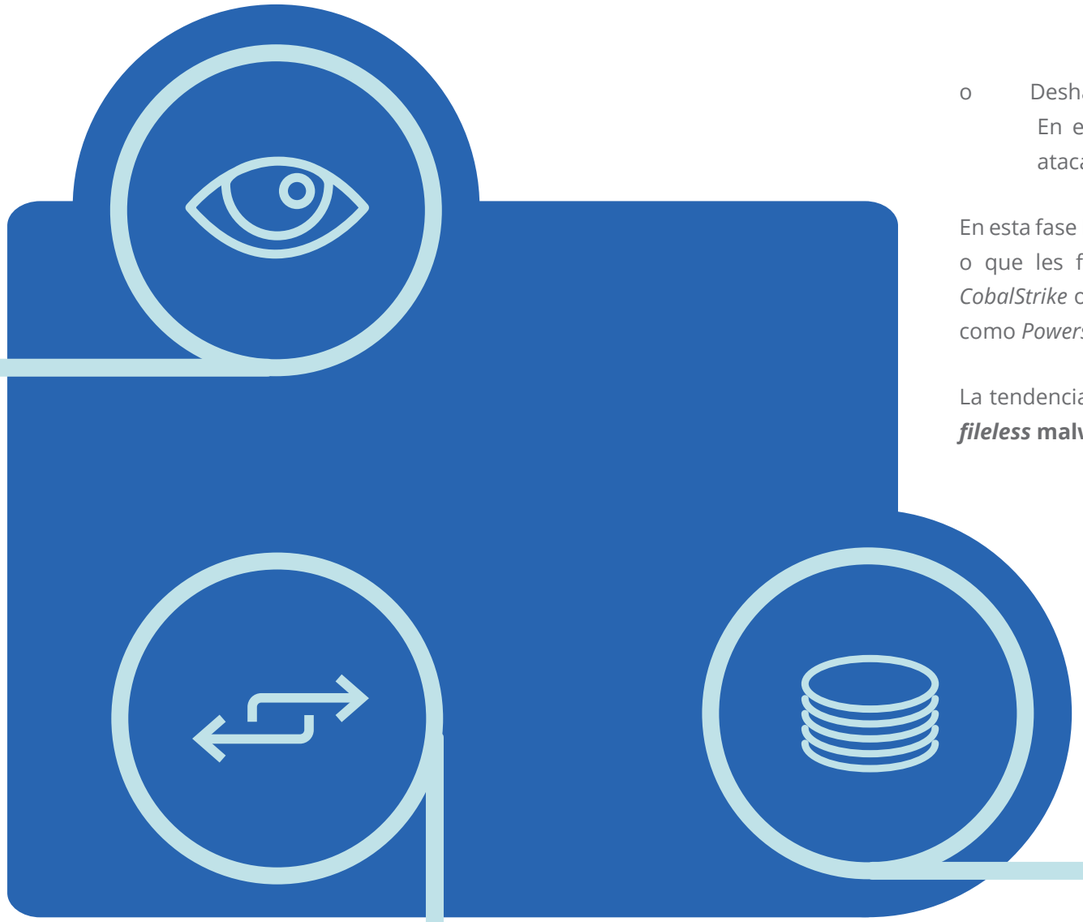
De forma muy resumida, el **modus operandi** en muchas de las actuales campañas de distribución de malware puede resumirse en:



Fase de intrusión | **Movimiento lateral** | **Explotación o colonización**

48 Véase https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cada una de estas fases puede modelarse tomando como referencia las **matrices de Tácticas, Técnicas y Conocimiento Común de Adversarios de ATT&CK**[49] y pueden servir de base para establecer el plan de salvaguardas.



Fase de intrusión

Los principales **vectores de entrada** que se están observando por parte de los atacantes son el **correo electrónico** y **servicios no seguros expuestos**.

En el caso del correo electrónico, habitualmente se trata de correos dirigidos a una o varias víctimas con un documento malicioso adjunto (generalmente haciendo uso de macros para la descarga del código dañino) o persuadiendo al usuario para que visite una web previamente comprometida; una vez allí, una falsa actualización del navegador, la instalación de complementos o mecanismos similares logran la descarga de la primera etapa (*stage*) del malware.

Por su parte, los servicios expuestos a Internet son una vía de entrada muy usada por los atacantes; servicios como RDP o SSH, que permiten acceso directo a la red interna, son atacados en busca de credenciales débiles o vulnerabilidades conocidas

Fase de movimiento lateral

Una vez dentro de la organización, los atacantes buscan ganar **persistencia** y **desactivar los sistemas de defensa**. Una vez asegurada la persistencia, la **propagación del malware** dentro de la organización se lleva a cabo utilizando diferentes **tácticas/técnicas**:

- Explotando vulnerabilidades conocidas (EternalBlue, EternalRomance, BlueKeep, etc.) que ayuden al movimiento lateral del atacante, como son las que afectan a protocolos como SMB.

- Robando credenciales y creando nuevos usuarios de administración.

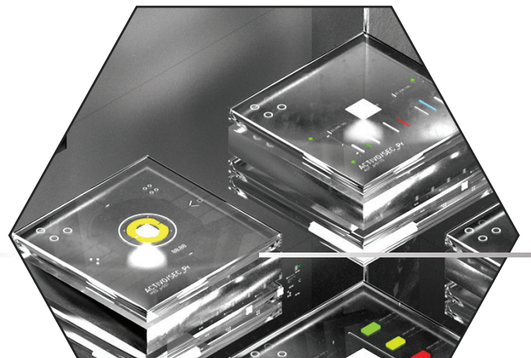
- Deshabilitando cualquier sistema de protección implementado. En el caso de que el interés sea distribuir un ransomware, los atacantes eliminarán también cualquier backup.

En esta fase los atacantes suelen usar **herramientas de post-explotación** o que les faciliten la propagación lateral, como por ejemplo *Empire*, *CobalStrike* o *Metasploit*, además de herramientas nativas de los sistemas como *Powershell*, *Batch Scripts*, *PSEXEC*, etc.

La tendencia es que las técnicas de ***Living off the Land*** (LOL) o el uso de ***fileless* malware** sean las más elegidas por los delincuentes.

Fase de explotación o colonización

Una vez obtenido el control sobre la infraestructura víctima, y establecido contacto con el sistema de Comando y Control, el atacante envía las **órdenes de descarga** y **detonación del malware** elegido, o bien cualquier otro tipo de acción a realizar sobre la red o sistemas víctima: exfiltración de información, alteración o eliminación de datos, cifrado, etc.



49 Véase https://attack.mitre.org/versions/v7/matrices/enterprise/

5.2.1 Vigilancia y auditoría continua

Bajo la premisa de que no es posible vigilar ni auditar aquello que no se ve, la primera iniciativa para vigilar las redes corporativas es medir la **superficie de exposición**. Esto incluye conocer los dispositivos conectados y el mayor detalle posible asociado a estos.

Es fundamental tener una **visibilidad** de todos los activos conectados a la red corporativa que componen la superficie de exposición sin importar el origen de las conexiones (cable, Wi-Fi o de forma remota). Deben existir entonces mecanismos implementados que permitan el descubrimiento del activo en el momento de la conexión antes de otorgar acceso al sistema.

Las principales salvaguardas tecnológicas para paliar los efectos de un ataque comienzan por la **monitorización de la infraestructura bajo vigilancia**. Implementar un **sistema de gestión** que incluya la **monitorización** y **correlación de alertas de fuentes** como firewalls, controladores de dominios, IDS, HIDS, etc. es fundamental, así como el despliegue de *endpoints* y herramientas anti-APT ayudarán a los analistas a detectar cualquier Táctica Técnica o Procedimiento (TTP), Indicador de Compromiso (IOC) o comportamiento anómalo que pudiera ser un indicio de compromiso.

La visibilidad completa, en conjunto con la vigilancia y auditoría continua, otorgan al organismo información que le permite identificar **vulnerabilidades** y **anomalías** para mitigar riesgos, bien sea de manera preventiva reduciendo la probabilidad de ocurrencia o controlando el impacto.

Es importante también revisar de forma periódica y monitorizar las conexiones con terceros, en particular las **VPN *site-to-site*** activas. Esto incluye establecer un protocolo de trabajo con cualquier tercero que legítimamente conecte con nuestra red corporativa, de forma que se garanticen unos requisitos mínimos de seguridad. Como se ha comentado anteriormente, los ataques a la cadena de suministro son una vía de entrada muy exitosa para los atacantes.

Cualquier sistema que preste un servicio avanzado de protección en el perímetro, tales como los antivirus, los EDR (Endpoint Detection and Response), los cortafuegos o los sistemas antispam, deben estar continuamente monitorizados y, de forma periódica, ser sometidos a una auditoría que corrobore que las reglas que tienen implementadas cumplen con sus objetivos. Dada su criticidad, otro servicio que debe estar continuamente monitorizado y bastionado es el **Directorio Activo**, que proporciona información sobre las actividades de todos los usuarios y sucesos del sistema.

Es necesario llevar un control exhaustivo del **estado de las actualizaciones de seguridad**, tanto en servidores como en equipos cliente, y

protocolos antiguos que presenten vulnerabilidades conocidas deberían ser eliminados, o cuando esto no es posible, protegidos por medidas compensatorias o complementarias de vigilancia adecuadas. Por ejemplo, no se debería utilizar autenticación LM/NTLM, y en el caso de que sea estrictamente necesario su uso por razones del negocio (compatibilidad, sistemas *legacy*, etc.), deben existir mecanismos de seguridad complementarios.

Otro ejemplo de reducción de superficie de ataque sería el de prohibir la habilitación de las macros en todos los documentos de Office, y plantear alternativas como el uso de las Localizaciones Confiables de Office para aquellos usuarios que realmente hagan un uso legítimo de ellas.

5.2.2 Establecimiento de doble factor de autenticación (2FA)

Zero Trust es un enfoque de seguridad de redes que invita a **eliminar la confianza** otorgada a todos los elementos que interactúan con la infraestructura del organismo y la forma en que lo hacen.

Este enfoque es la respuesta natural para la gestión del riesgo en un contexto en donde la tendencia de las redes corporativas incluye, entre otros, usuarios remotos, activos e información en la nube, servicios subcontratados o proveedores remotos.

En el modelo Zero Trust se puede decir que cuando se habla de usuarios, la validación de identidades es una iniciativa obligatoria y debe ser lo más estricta posible. Antes de otorgar cualquier acceso o realizar cualquier consumo de recursos corporativos, el usuario deberá ser autenticado.

Autenticar, en un contexto de validación de identidades, es un control que procura confirmar que alguien es quien dice ser, la validación de identidad se puede realizar de **tres (3) formas distintas**:

- Algo que el usuario sabe.
- Algo que el usuario tiene.
- Algo que el usuario es.

Establecer un **segundo factor de autenticación** (2FA), significa usar dos (2) formas de validación de identidad antes de que un usuario pueda considerarse autenticado. Por lo general, el primer factor de autenticación usado son las credenciales corporativas de usuario *(Algo que el usuario sabe)*. Como segundo factor a menudo se usa un código de validación enviado a un dispositivo asociado al *usuario (Algo que el usuario tiene)*.

Se recomienda establecer 2FA para servicios críticos que estén accesibles desde fuera de la organización, ya se trate de conexiones remotas vía VPN, correo electrónico, sistemas en la nube, etc.

Del mismo modo, aquellas acciones críticas que puedan suponer un alto impacto para la organización (acceso a servicios críticos, a información sensible, transferencias económicas cuantiosas, etc.) deberían requerir un segundo factor de verificación.

5.2.3 Control de permisos de los usuarios

El establecimiento y control de permisos de usuarios en la red corporativa deberá regirse bajo el principio del **mínimo privilegio**, es decir, otorgar a los usuarios los permisos específicos que requiere para el desempeño de su rol y la ejecución de sus funciones en el organismo: ni un permiso más, ni un permiso menos. Para lograr este objetivo, se deben articular diferentes iniciativas internas que no solo tienen un carácter tecnológico.

Es importante que los organismos definan correctamente dichos roles y las funciones de cada miembro del mismo. Esto vincula una identidad corporativa a un conjunto de actividades. Las **actividades**, a su vez, cuentan con ciertos **requisitos** o se realizan sobre unas determinadas **herramientas tecnológicas** tales como aplicaciones corporativas, portales web de la intranet, sitios remotos en internet, etcétera. Los requisitos para la ejecución de las actividades ligadas a cada rol determinarán los permisos de acceso necesarios habilitados para cada uno de ellos para cada identidad encargada de ejercer el rol en cuestión.

El principio de mínimo privilegio es una iniciativa teórica que requiere alineamiento y coordinación entre varios elementos del organismo antes de ser una realidad puesta en práctica. Tecnológicamente, este principio se puede implementar apoyado sobre diferentes plataformas tales como una base de datos de usuarios corporativos, una herramienta de control de acceso a la red (NAC), un firewall, una estrategia de segmentación o un proceso de establecimiento de identidad adecuado. Este principio se encuentra estrechamente ligado a la gestión de identidades. En un primer lugar, es importante establecer la **identidad del usuario** para posteriormente asignar los **permisos de acceso** correspondientes.

Los usuarios no deberían ser administradores de los equipos bajo ningún concepto, de la misma forma que no se debería usar la misma contraseña de administración en toda la organización.

Para minimizar este riesgo, una solución adecuada es hacer que la contraseña de administración de cada equipo sea distinta y que cambie de forma periódica.

5.2.4 Segmentación de red

Segmentar la red supone **dividir la superficie de ataque**. Una vez se toman las medidas de seguridad para el control de la superficie de exposición, estas se encontrarán mejor acotadas, los segmentos se podrán proteger de manera optimizada y se creará una barrera virtual entre segmentos de red. Estos son sólo algunos ejemplos de los beneficios de la segmentación. Los organismos están llamados a tener estrategias de segmentación bien definidas, ya que representan el diseño orientativo que ha de seguir su red ante el crecimiento y la necesidad de escalar.

Segmentar la red consiste en encontrar la forma más apropiada de **dividir** en partes más reducidas toda la **superficie de ataque dispuesta en la organización**. Para segmentar la red, es necesario contar con la infraestructura tecnológica que soporte la estrategia de segmentación elegida. Por lo general, se tienen en cuenta varios criterios para elegir la forma de segmentar la red. No obstante, es necesario tener en mente que el riesgo, la criticidad de los activos o su función, entre otros, son temas a considerar que determinan cómo debe dividirse la red.

Existen marcos de referencia de buenas prácticas y recomendaciones de fabricantes de equipos de telecomunicaciones que sugieren formas de segmentación de redes. Es evidente que cada red de cada organismo tiene su propia caracterización y, por ello, resulta complejo estandarizar un modelo único de segmentación.

Es necesario implementar una **segmentación de red adecuada**, en la que se incluya un equipo concentrador de salto desde el que los administradores puedan acceder a los equipos a administrar. En este caso, es crítico que el equipo concentrador de salto haya sido específicamente bastionado para esta función, y se hayan definido claramente las políticas a seguir para determinar quién está autorizado para acceder a qué equipos desde sistema.

Otras políticas aún más restrictivas serían el uso de **PaW** (*Privileged Access Workstations*), puestos bastionados que solo se usen para administrar los sistemas, o requerir que el acceso a los servidores se realice exclusivamente a través de máquinas de salto.

5.2.5 Auditoría de Powershell

PowerShell es una potente **herramienta de línea de comandos** y un **lenguaje de scripting** que viene instalada por defecto en un gran número de entornos **Windows**, que en la actualidad es muy utilizada para la ejecución de código malicioso en entornos Microsoft. Debido a que, por defecto, genera pocas pistas de su ejecución, presenta grandes ventajas para los atacantes, ya que dificulta identificar que un sistema está siendo atacado, así como el análisis posterior de los ataques.

De hecho, en las primeras versiones de *PowerShell* únicamente quedaba registrada la ejecución de una *shell*, pero no las acciones registradas. Microsoft ha ido mejorando este problema, sobre todo a partir de la versión 5.0, y ahora cuenta con herramientas potentes para la creación de registros/*logs*.

Las tres (3) principales herramientas para la creación de *logs* que ofrece *PowerShell* son *Module Logging*, *Script Block Logging* y *Transcription*.

5.2.6 Protección frente a ataques Pass-the-Hash

Pass-the-hash es una técnica que permite a un atacante autenticarse en un servidor o servicio remoto utilizando el hash de NTLM de la contraseña de un usuario, en lugar de requerir la contraseña en texto plano como es normalmente el caso. De este modo, para el atacante ya no es necesario obtener la contraseña en texto plano.

Algunas **recomendaciones** en este sentido, de forma muy general, son las siguientes:

- Priorizar las máquinas y cuentas más críticas que pueden tener una mayor probabilidad de ser el objetivo de un ataque.
- Identificar el comportamiento normal.
- Diseñar una defensa contra el robo de credenciales, mediante un protocolo de uso y almacenamiento de credenciales que verifique la seguridad de la transmisión.
- Diseñar e implementar normas para los administradores de sistemas y redes.
- Bastionar y restringir los hosts utilizados para propósitos de administración de la infraestructura o los usuarios.
- Implementar una adecuada segmentación de la red.
- Diseñar, implementar y monitorizar la aplicación de unos procedimientos establecidos formalmente para garantizar un uso aceptable de los activos de la organización.
- Implementar herramientas que permitan o faciliten la detección del uso de credenciales robadas.

5.2.8 Simulacros/ Ciberejercicios

Es interesante llevar a cabo simulacros periódicos de ciberincidentes, lo más reales posible, para **poner a prueba los procedimientos y entrenar la capacidad de reacción de los equipos**, así como mejorar la capacidad de respuesta ante incidentes.

Este tipo de ejercicios permiten reforzar la coordinación interna interdepartamental y entre entidades, además de servir como herramienta para mejorar la concienciación entre el personal implicado, que no siempre está directamente implicado en la gestión de la seguridad.

5.2.9 Copias de Seguridad

Hacer **copias de seguridad** de toda la información relevante en una o más ubicaciones diferentes a la que se encuentran los sistemas de información principales sigue siendo una de las principales medidas de protección.

Para ello, es necesario que al menos una de dichas **copias** sea **off-line**, y muy preferiblemente se encuentre cifrada.

La recopilación de copias de seguridad puede resultar una tarea ardua si no se cuentan con las herramientas tecnológicas pertinentes que permitan agilizar y optimizar dicha recolección. Las herramientas de centralización son fundamentales para la ejecución de este tipo de tareas operativas: automatizan gran parte de la labor y permiten una ejecución trasparente y adecuada.

5.2.7 Contrainteligencia/ Engaño

El despliegue de sistemas de contrainteligencia basados, por ejemplo, en *honeypots*, *honeynets*, *honeytokens*, etc. proporciona información muy valiosa para estudiar los patrones de comportamiento de los atacantes, a la vez que se evita que accedan a entornos reales.

5.3 Salvaguardas conductales

El necesario equilibrio entre **usabilidad** y **ciberseguridad** en el uso de la tecnología y el manejo de información provoca que mantener un adecuado nivel de ciberseguridad en las organizaciones requiera una adecuada **implicación de las personas**.

Como ha sido analizado en los puntos anteriores, los agentes de la amenaza son conscientes de esta realidad y sacan partido de ella utilizando a las personas como vector de entrada de sus ciberataques, haciendo uso de todo tipo de **prácticas de ingeniería social**: *phishing*, *smishing*, *vishing*, *media dropping*, etc. A esto hay que sumarle las **brechas de ciberseguridad** (por ejemplo, fugas de información) producidas por descuidos y prácticas inseguras adoptadas por los empleados.

Esta situación provoca que los departamentos de ciberseguridad consideren a las personas como un elemento crítico en su estrategia de protección, acuñando la famosa frase "**las personas son el eslabón más débil de la cadena**". No obstante, al igual que la conducta insegura de las personas introduce riesgos en la organización, una conducta segura puede convertirse en una salvaguarda muy efectiva: **salvaguardas conductuales**.

Por todo ello, resulta indiscutible la necesidad de trabajar en la dimensión de las personas, con el objetivo de mejorar el nivel de ciberseguridad en las organizaciones, y así lo reflejan los principales marcos legales y normativos en materia de ciberseguridad tanto a nivel nacional como internacional como son la **Estrategia Europea de Ciberseguridad**, la **Estrategia Nacional de Ciberseguridad**, el **Esquema Nacional de Ciberseguridad**, y la **norma UNE-ISO/IEC 27002:2013 (Cor.2015)** -Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.


EUROPEAN COMMISSION

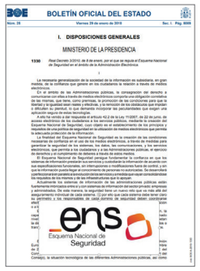
HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

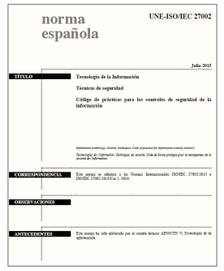
An Open, Safe and Secure Cyberspace


BOLETÍN OFICIAL DEL ESTADO

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

ens
Esquema Nacional de Seguridad


norma española

UNE-ISO/IEC 27002

Julio 2015

TÍTULO

Tecnología de la Información

Técnicas de seguridad

Código de prácticas para los controles de seguridad de la información

CORRESPONDENCIA

ANÁLISIS NACIONAL

ANTECEDENTES

El objetivo final del proceso es el **incremento del nivel en ciberseguridad**, conseguido mediante la mejora de la cultura en ciberseguridad de la organización, que en última instancia se define a partir de la conducta de cada una de las personas que forman parte de esta.

5.3.1 Plan estratégico de mejora del nivel de la cultura en ciberseguridad

Para lograr dicho objetivo, resulta muy conveniente, casi necesario, el diseño y puesta en marcha de un plan estratégico de mejora del nivel de la cultura en ciberseguridad, que promueva los **cambios en la conducta de las personas** mediante la realización de **acciones de concienciación y formación en ciberseguridad.**

Por su parte, las **acciones de concienciación** tienen como objetivo involucrar e implicar a las personas en la gestión de la ciberseguridad, ayudándoles a entender la importancia de su rol como parte activa de la estrategia de protección.

Por otro lado, las **acciones formativas específicas** permiten trasladar a las personas el conocimiento necesario para adoptar prácticas de comportamiento seguro que conduzcan a una gestión adecuada de los riesgos que les competen.

Si nos centramos como ejemplo en la gestión del riesgo asociada a las amenazas que utilizan la ingeniería social como vector de entrada, una salvaguarda conductual efectiva pasaría por lograr que los empleados conozcan:

- la amenaza y su papel en la gestión del riesgo asociado;
- las pautas para identificar un ataque de ingeniería social en sus distintas vertientes;
- cómo actuar cuando los detectan y cómo reportar de forma activa al equipo de ciberseguridad.

Al igual que ocurre con cualquier otra salvaguarda de ciberseguridad, es necesario que estos planes incorporen mecanismos de medición que permitan conocer la **eficacia** de las medidas desplegadas.

En esta línea, es posible clasificar los planes de mejora de la cultura de ciberseguridad por su **nivel de madurez**, atendiendo al **alcance** y **tipología de acciones** abordadas en los mismos.

5.4 Salvaguardas procedimentales

5.4.1 Vigilancia y auditoría continua

A continuación, se enumeran una serie de **actividades** fundamentales para la **vigilancia** y **auditoría continua** de la superficie de exposición:

1. **Descubrimiento del 100% de todo lo conectado:** No podemos vigilar ni auditar lo que no vemos. La primera iniciativa para vigilar las redes corporativas es conocer la superficie de exposición en su totalidad. Esto incluye conocer los dispositivos conectados y todo el detalle asociado a los mismos: conocer la tipología de los dispositivos permite la caracterización de los activos y, por consiguiente, determinar el riesgo asociado a cada uno de ellos.

Nuevos dispositivos: descubrir y conocer todos los dispositivos conectados en la red, locales y remotos.

Nuevos puntos de conexión: identificar el tipo de acceso de cada conexión realizada en la red (cableada, Wi-Fi, VPN).

2 **Perfilado de los dispositivos:** hace referencia a la capacidad de caracterizar cada activo vinculado a cada conexión que se realiza en la red. Esta capacidad otorga un conocimiento mayor y, por ende, la estimación de riesgo resulta más precisa.

Información básica de conexión: dirección IP, MAC.

Información de la categoría del dispositivo (tipología): por ejemplo, teléfono, desktop, laptop, cámara, etc.

Criticidad del dispositivo: a partir del perfilado, se puede realizar la evaluación de riesgo asociado a cada dispositivo.

Requisitos mínimos de conexión: una vez conocidas las características del dispositivo asociado a cada conexión, es posible exigir requisitos mínimos de conexión (por ejemplo, que el equipo cuente con un antivirus, determinados parches del sistema operativo, etc.).

3 **Aseguramiento de superficie:** con todo el conocimiento de las conexiones, es posible determinar los controles o las medidas de seguridad que han de aplicarse en cada caso para mantener los valores de riesgo.

Uso de VPN: se utiliza, por lo general, en conexiones remotas para generar túneles virtuales privados sobre infraestructura pública.

Protocolos cifrados: las conexiones remotas, e incluso para los servicios web, deberían usar HTTPS para asegurar los datos intercambiados en cada conexión.

Control remoto: las conexiones remotas requieren vigilancia y auditoría continua de manera que se pueden identificar y prevenir los comportamientos anómalos.

i. **Comprobación de postura:** se refiere a la validación de requisitos mínimos de conexión exigidos al dispositivo de usuario usado en el establecimiento de la conexión.

ii. **Monitorización de tráfico de usuarios remotos:** es importante mantener una vigilancia continua sobre el tráfico asociado a cada conexión con el fin de identificar cualquier comportamiento anómalo. A partir de ello, es posible tomas las acciones que correspondan en cada caso.

5.4.2 Establecimiento de 2FA (Zero Trust)

Como se ha comentado en puntos anteriores, la iniciativa de validar identidades de manera estricta con el objetivo de mantener la red segura para usuarios remotos, la implementación del **doble factor de autenticación (2FA)** es crucial en estos casos.

A continuación, se detallan algunas **actividades** para llevar a cabo esta tarea.

1 **Establecimiento del primer factor de autenticación:** a menudo el primer factor de autenticación evalúa algo que *el usuario sabe*. En la mayoría de las ocasiones, esto se realiza a través de las credenciales de usuario corporativo (nombre de usuario y contraseña).

Definición de credenciales de usuario corporativo: los organismos tienen las identidades corporativas centralizadas en una base de datos de usuarios (AD, LDAP, entre otros).

Vinculación de base de datos de usuarios a plataforma de acceso: La base de datos de usuarios corporativos debe vincularse a la plataforma de control de acceso para que sean consultada cada vez que se quiera acceder a la red corporativa.

2 **Establecimiento del segundo factor de autenticación:** Los organismos deben contar con una herramienta tecnológica que les permita desplegar un segundo factor de autenticación. Frecuentemente se utiliza como segundo factor de autenticación algo que está vinculado a la identidad del usuario (*algo que el usuario tiene*). Usualmente se trata de un dispositivo móvil, como el teléfono u otro que le permita recibir un código que sea usado como segundo factor de autenticación.

Despliegue de plataforma para segundo factor de autenticación (2FA): las plataformas más conocidas de segundo factor de autenticación envían un código conocido como ***one time password*** **(OTP)** al móvil del usuario. Estos códigos tienen una vigencia temporal corta (de unos 60 segundos aproximadamente). El tiempo de vigencia de dicho OTP será el tiempo durante el cual el código esté disponible para una autenticación exitosa.

Vinculación de 2FA a plataforma de acceso: la plataforma de 2FA debe vincularse a la plataforma de control de acceso encargada de orquestar la autenticación de las conexiones. El usuario deberá ingresar el segundo factor de autenticación para validar su identidad cada vez que quiera acceder a la red corporativa.

3 **Acceso con doble factor de autenticación:** tras implementar los dos factores de autenticación, el usuario deberá introducir, en primer lugar, sus credenciales corporativas *(algo que sabe)* para posteriormente introducir el segundo factor *(algo que tiene)*. Por lo general, el segundo factor de autenticación se implementa para conexiones remotas tales como las que realizan usuarios internos y externos por medio de VPN.

5.4.3 Control de permisos de los usuarios (Autorización, Principio de Mínimo Privilegio)

Para otorgar a los usuarios los permisos específicos que requieren para el desempeño de su rol y la ejecución de sus funciones en el organismo, deben articularse diferentes **iniciativas** dentro de dicha organización no solo de carácter tecnológico, sino también relacionados con la estructura y funcionamiento del organismo. A continuación, se describirán una serie de **actividades** clave que permitirán el establecimiento del principio de mínimo privilegio de **forma práctica**:

1 **Establecimiento de identidades corporativas:** el principio del mínimo privilegio está estrechamente ligado con la gestión de identidades. Es importante, en un primer lugar, establecer la identidad del usuario para posteriormente asignar los permisos de acceso correspondientes.

Usuario y credenciales corporativas: los organismos deben contar con una base de datos de usuarios (LDAP, AD, entre otros). Esta base de datos almacenará la información de los usuarios (usuario y contraseña), y será el servidor para consultar durante los procesos de autenticación para el acceso de los usuarios.

Procesos de autenticación: determinar el proceso de autenticación para los accesos de usuarios depende de diferentes cuestiones. Por ejemplo, el tipo de usuario (externo o interno), el lugar de conexión (local o remoto), etcétera.

A menudo, los procesos de autenticación se realizan por medio de un único factor de autenticación cuando se trata de un usuario interno y se realizan de forma local en el organismo, implementándose el doble factor de autenticación (2FA) principalmente para conexiones remotas. Para el caso remoto en particular, se deberá entonces contar con una herramienta tecnológica que permita el establecimiento de doble factor de autenticación (2FA).

2 **Determinación de permisos de acceso para cada rol:** cada rol del organismo tiene asociada una serie de funciones. La ejecución de estas funciones se apoya sobre recursos tecnológicos (como, por ejemplo, servidores, aplicaciones, entre otros). Se deberá, entonces, vincular cada función de cada rol a un recurso en la red para, a partir de ello, establecer los permisos que requiere cada identidad corporativa en la red.

Roles y funciones corporativos: existen diferentes tipos de roles en las organizaciones. Sin embargo, por ejemplo, dependiendo del caso muchas veces existen roles operativos que realizan las mismas funciones, pero son ejecutados por personas distintas. El organismo deberá tener un manual de funciones por rol y estas deben asociarse con recursos tecnológicos que soporten su ejecución.

Identificación de recursos tecnológicos: los recursos tecnológicos son aquellos elementos que se requieren para la ejecución de tareas corporativas, (por ejemplo, servidor de correo, herramienta de ticketing, intranet, etc.). Cada recurso tecnológico tiene un objetivo y realiza en sí mismo una función. Los organismos deberán conocer cada recurso y su función específica.

3 **Estrategia de segmentación de red:** existen marcos de referencia de buenas prácticas de segmentación de redes. A pesar de que cada red corporativa cuenta con su propia caracterización y resulta complejo estandarizar un modelo único, hay segmentos de red que deben estar definidos (por ejemplo, campus, datacenter y edge). A partir de ello, elaborar un diseño escalable y ordenado de la red local será una tarea de crecimiento más sencilla y estandarizada.

4. **Gestión de acceso:** esta gestión demanda la articulación de varias plataformas y genera un proceso definido que permitirá estandarizar la seguridad de los accesos en la red independientemente de su naturaleza.

Articulación de plataformas tecnológicas: la primera iniciativa aquí es el establecimiento de identidad. Se realiza mediante una plataforma de autenticación de uno o dos factores que consulte los datos del usuario en la base de datos de usuarios del organismo.

Posteriormente, la determinación del rol asociado a la identidad permitirá establecer los accesos definidos y los recursos tecnológicos necesarios para la ejecución de las funciones de cada rol. Los accesos permitidos determinan los flujos a habilitar para cada usuario y con ello, permite a los usuarios y dispositivos interactuar con los servicios de red que correspondan para cada caso: ni uno más, ni uno menos.

5.4.4 Segmentación de red (Campus / Core / Edge / Datacenter, Aislamiento)

Conocer los activos y servicios dispuestos en la red corporativa, así como la forma en la que se consumen, es un requisito fundamental para definir en un primer lugar los segmentos y posteriormente la ubicación de los activos y servicios corporativos. Existen **modelos estándar, buenas prácticas de segmentación**, incluso **recomendaciones de fabricantes** para determinar los segmentos de red. Dentro de los modelos de segmentación conocidos existe uno que separa **tres (3) ambientes**:

1. **Campus:** segmento de red donde se encuentran los usuarios y dispositivos de red como impresoras, cámaras, teléfonos IP, etc.

2. **Datacenter:** segmento de red que aloja los servidores corporativos. Por lo general, este segmento concentra la mayor cantidad de tráfico de la red.

3. **Edge:** segmento donde se encuentran algunos servicios corporativos publicados en internet. También se conoce como DMZ.

El reconocimiento de estos tres (3) segmentos de red es una actividad importante cuando se comienza a establecer una **estrategia de segmentación**. A continuación, se detallará una serie de actividades que permitirán ejecutar una segmentación de red adecuada.

1. **Conocer la superficie de exposición:** el reconocimiento de la superficie de ataque es fundamental para determinar la estrategia de segmentación. Antes de empezar a dividir la superficie es necesario conocer la **extensión** de la misma.

Inventario de servicios de red: es necesario conocer qué y cuántos servicios de red corporativos existen. Por ejemplo, es necesario conocer con claridad si existen servicios de conexión remota.

El conocimiento de los servicios permite determinar parte de la superficie de ataque a partir de la forma en la que se consumen.

Conocimiento de flujos de comunicación: los servicios de red son expuestos interna y/o externamente. Esta información es determinante para establecer la superficie de exposición.

Partiendo de esta información, es posible establecer la ubicación de los recursos del organismo y la forma más segura en la que deben interactuar con los demás activos y usuarios de la organización.

2 Definir la estrategia de segmentación a seguir: por lo general, la estrategia de segmentación elegida sigue guías de buenas prácticas conocidas. La definición de los ambientes de Edge, Campus y Datacenter es una de esas guías.

Una vez definidos los ambientes, se debe procurar un proceso de **optimización** propio de cada organismo donde se aplique la segmentación que beneficie la articulación de los servicios y la forma en que se consumen.

Elegir el diseño y los ambientes: con frecuencia el diseño de una red corporativa es establecido en un momento inicial pensando en brindar ciertos servicios en el corto plazo más que en un crecimiento o incremento de servicios de red.

La topología se hereda y los cambios se evitan, llevando a cabo simplemente ajustes menores, ya que, para entonces, un cambio de arquitectura de red representa un gran impacto para la operación de los organismos.

Sin embargo, cada día las **buenas prácticas** son aplicadas con mayor frecuencia. Además, los requisitos propios del crecimiento y expansión de los organismos demandan una reorganización de la infraestructura que le permita ajustarse a las condiciones de crecimiento, apertura y madurez tecnológica.

A día de hoy, en la mayoría de las redes corporativas podemos diferenciar tres (3) ambientes: Campus, Edge y Datacenter. Partiendo de esa base, cada organismo cuenta con una segmentación de usuarios y dispositivos IoT y servicios publicados en internet propios, además de servidores corporativos que responden a las agrupaciones propias de cada organismo.

Optimizar la arquitectura de red: una vez establecidos los segmentos de red, se deben comenzar con los **procesos de optimización**. Los flujos de consulta de servicios corporativos serán de gran utilidad para optimizar el consumo de recursos y en general del tráfico de red (la optimización para la prevención de latencias, exposición de servicios críticos, entre otros).

Muchas vulnerabilidades pueden ser mitigadas partiendo de una buena estrategia de segmentación de red.

5.4.5 Copias de Seguridad (Centralización)

Con frecuencia, los organismos adoptan **estándares de buenas prácticas** que incluyen **directrices de recolección de copias de seguridad**. El trabajo de cada organismo es seguir dichas directrices de la mejor manera posible con el apoyo de la tecnología que corresponda para facilitar su ejecución.

1 **Activos con copia de seguridad:** definir qué activos tendrán copias de seguridad es fundamental para determinar la forma en la que se van a recopilar dichas copias.

2 **Tiempos de almacenamiento de copias:** por lo general, las copias de seguridad tienen un tiempo de almacenamiento determinado con el objetivo de prevenir que el servidor de almacenamiento llegue al máximo de su capacidad.

Los tiempos de retención de las copias de seguridad están definidos por cada organismo, dependiendo generalmente del estándar aplicado y el almacenamiento disponible.

3 **Tiempos de ejecución:** las copias de seguridad son realizadas en horas de baja afluencia de tráfico. Generalmente, son actividades programadas que se realizan de manera automática a través de una herramienta de centralización capaz de realizar la tarea.

5.4.6 Capacidad adaptativa para operaciones seguras fuera del marco de actividad convencional

Es evidente que, durante períodos de pandemia como la crisis de la covid-19, muchos trabajadores han desarrollado su labor profesional desde sus domicilios particulares, haciendo uso para ello de sus propios **equipos domésticos**, también empleados para cuestiones personales, utilizando **aplicaciones propias**, ajenas a su desempeño profesional. En estos equipos lógicamente no se encuentran implementadas las medidas de **protección** y **seguridad** corporativas.

Las amenazas y escenarios no previsibles, como es la inclusión de vectores de amenazas propios de un sector más doméstico, pueden implicar la aparición de incidencias para las que sus sistemas de detección, alerta y protección podrían no estar preparados.

> Los planes de contingencia deben observar en sus medidas procedimentales y modelos de actuación la posible aparición de circunstancias imponderables, como el uso de equipos domésticos para labores profesionales.

Se establece por lo tanto la necesidad de evaluar **nuevos procedimientos** que puedan ser desplegados para operativas y escenarios de trabajo no habituales y que no suelen estar incluidos en los **planes de contingencia corporativos**.

De esta manera, los planes de contingencia deben observar en sus medidas procedimentales y modelos de actuación la posible aparición de **circunstancias imponderables** que pueden afectar de forma sensible a sus sistemas. Estos procedimientos deben regular la capacidad de adaptarse a diversas situaciones y facilitar su aplicación con la mayor inmediatez posible ante circunstancias imprevistas, no habituales y que posiblemente no se han contemplado de forma específica en los planes ya existentes.

Algunos **ejemplos de este tipo de procedimientos** podrían ser los siguientes:

- Operación en modo seguro fuera de los establecimientos de la organización.
- Puesta en marcha de medidas de protección que admitan un modo de operación de los sistemas de la información diferentes a las convencionales o a las que ya estén definidos en los planes de contingencia.
- Accesos remotos seguros que permitan extender las actividades laborales en entornos de baja confiabilidad.
- Comunicación al personal sobre cambios y adaptaciones a los procesos.
- Comunicación al personal de la necesidad de aplicar medidas eventuales de seguridad o en los procesos de tratamiento de la información.
- Establecer un protocolo de teletrabajo como procedimiento operativo, observando las consideraciones de seguridad.
- Soporte remoto seguro, para el entorno de teletrabajo.
- Evaluación de medidas de seguridad en sistemas de uso doméstico para la conexión y la operación en el entorno corporativo.

Se aconseja que las organizaciones exploren la identificación de otros posibles procedimientos siempre asociados a su modo de operación, prestación de los servicios y manejo de información.

5.4.7 Procedimientos de seguridad asociados a la estacionalidad

Resulta evidente que en períodos concretos o bajo situaciones cambiantes se dan condiciones que implican la necesidad de adoptar nuevos procedimientos y, por ende, aplicar medidas adicionales. Estos inicialmente solo son de aplicación durante un tiempo limitado hasta que se revierta a la situación habitual.

> El periodo navideño o épocas consumistas como el "Black Friday" puede ser aprovechado por los cibercriminales para incrementar el volumen de correos con contenido malicioso o de Spam.

Un ejemplo ilustrativo de este hecho puede ser el **periodo navideño**. Aunque ciertamente la actividad de las organizaciones tiende a mantenerse, el tipo de operaciones se modifica significativamente. En dicho periodo se incrementa significativamente el intercambio, más o menos profesional, de correos electrónicos con un componente emocional superior al que habitualmente conllevan los que se intercambian durante el resto del año.

Este hecho que resulta muy natural, puede ser aprovechado por los **cibercriminales** para incrementar el volumen de **correos con contenido malicioso o de Spam**. Es incuestionable que en este escenario se es más propensos a abrir determinados mensajes que en otras épocas del año probablemente generarían desconfianza.

Esta misma circunstancia puede coincidir también con épocas consumistas tales como el **"Black Friday"** o similares, donde los mensajes presentan ofertas muy competitivas, incluso de productos tecnológicos orientados a las organizaciones, pero que realmente esconden fines más oscuros.

Así será interesante para estas circunstancias preparar **procedimientos** que sean de aplicación solo bajo determinadas condiciones o en **épocas concretas** del año. Algunos procedimientos a observar podrían ser:

- Comunicación o concienciación al empleado ante fechas o situaciones específicas.
- Implementación de medidas de seguridad incrementales ante fechas o situaciones específicas.
- Implementación de medidas de operación de servicios o protección de información ante amenazas materializadas por situaciones estacionales.

5.4.8 Revisión del modelo de amenazas por cambios operacionales

En los meses de pandemia, se ha detectado un significativo incremento de mecanismos empleados para evadir los sistemas de protección *antiphising*. El objetivo lógicamente era impactar. Cuando no era factible hacerlo a través del correo profesional, se ha empleado para ello el correo personal. Esto es posible, cruzando información de redes sociales personales y/o profesionales.

De este modo, se ha apreciado un significativo aumento de correos procedentes de fuentes **cibercriminales** que emplean **técnicas más sofisticadas** que las tradicionales. Técnicas de *Bypass* usando caracteres de escape en hexadecimal, técnicas de *Zerofont*, *BaseStriker* u otras. Inclusive en ataques más dirigidos ha podido utilizarse la lógica de que un mismo equipo puede ser potencialmente empleado por más de una persona del núcleo familiar. Pudiendo así ser más fácil impactar a través del correo del miembro menos concienciado pero usuario del equipo.

Es posible en ese sentido, que los análisis de riesgos puedan determinar bajo determinadas condiciones de trabajo, que los usuarios deben prestar su actividad de forma distinta cuando se encuentren actuando en un entorno doméstico o cuando empleen equipos no corporativos. En este tipo de escenarios, puede no ser recomendable el manejo de la información más sensible, a diferencia de lo que el profesional haría encontrándose en su puesto de trabajo habitual.

No solo es necesario que los equipos de seguridad de las organizaciones sean conscientes de estas problemáticas, es también necesario evaluar las nuevas amenazas y plantear **mecanismos de protección debidamente procedimentados**, reduciendo potenciales riesgos y amenazas, así como el impacto que estas pueden producir.

Es por ello, que se plantea la necesidad de procedimentar las siguientes **acciones**:

- Evaluación de amenazas que evolucionen según circunstancias.
- Incluir activos ajenos a la organización pero que pueden interactuar con esta.
- Incluir modelos de entornos fuera del lugar de trabajo y con seguridad física no adecuada.

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

CCN
centro criptológico nacional